REMARKS

Claim 1 is presented in amended form. Thus, by this Amendment, Claims 1 through 24 as amended are again presented for examination.

The Examiner has rejected all claims of the application as filed. Claims 1 through 16, 21 and 23 are rejected as allegedly rendered obvious by the International application of Schultz et al. in view of the United States patent of Carter. Claims 17 through 20 and 22 are rejected are rejected as allegedly obvious on the basis of the foregoing combination further in view of the United States patent of Chen et al. Finally, Claim 24 is rejected as obvious on the basis of Schultz et al. in view of Carter further in view of the Untied States patent of Auerbach et al. For the reasons set forth below, it shall be clear that the basic reference, Schultz et al., is so readily distinguishable from the claimed invention as to render each of the pending rejections unsupportable.

The pending office action is difficult to interpret as the Examiner has made only cursory comments that purport to relate limitations of Claim 1 the main reference, Schultz et al. Rather than attempt to respond by offering a similarly-opaque critique of the Examiner's position, it will be helpful, and illuminative of the significant conceptual distinctions that

exist between the claimed invention and the primary reference to provide side-by-side analyses of the two systems.

The claimed invention is directed to a method for secured access to data in a network. Such method is illustrated in the application with reference to the secure access to patient medical records among providers. However, the invention is not limited to medical applications. In the claimed invention, a plurality of data area access systems are provided, along with, and separate from, an information center. Patient data is stored only once (i.e. at the data access center where such data was generated, subject to the patient's approval). A record of the existence and location of such patient data (i.e., the particular data area access system where it is stored) is transmitted to and kept only at the information center. The data owner (i.e. the patient), provides inputs that are transmitted to the information center that identify which data area access systems (e.g. doctors) are entitled to access to which records maintained at the information center. Thus, not all doctors on the network are entitled even to learn of the existence of patient data stored at a remote data area access system.

Once a request for patient records is received at the information center from a data area access system, the information center, upon verification of the request, will

provide information indicating the existence of medical records (but not the underlying data, such as x-rays) upon verification of a data area access system user code. The information provided by the information center to the qualified data area access system will include the identity of the data area access systems where particular patient information is stored. Figure 5 of the application and the accompanying written description illustrate the process whereby data transfer within the invention proceeds among data area access systems subject to continuous user verification steps. Such step-by-step verification, and the consequent high security, follows from a combination of the arrangement and protocols of the claimed invention.

In contrast to the system of the claimed invention, in which confidentiality is guarded through the dispersal of information (i.e. data limited to a single data area access system, listing of data kept in the system to a information center separate from any other data area access system, etc.) coupled with a system of access codes that serve to limit the access of a user strictly in accordance with the wishes of the data owner (the patient, see Figure 5 of the pending application), Schultz et al. teaches a network-based system that for making the medical data of a patient-subscriber accessible to authorized physicians through a computer network. In contrast to the dispersed system of the claimed invention, in Schultz et al.

medical information of a patient-subscriber is assembled into a single Global Electronic Medical Record (GEMR) that is stored on the patient-subscriber's GEMR server. The patient-subscriber's GEMR server is addressable on the computer network of Schultz et al. In contrast to the claimed invention in which the rights of particular data area access systems is entered into the information center by the data owner himself (not necessarily with the knowledge of the data access center), access to the data of a patient's GEMR (password and address) is obtained by the straightforward process of delivery of password and network address information to the physician from the subscriber-patient. This extremely significant difference between the primary reference, which is not met by the reference to the Carter reference, is set forth at subparagraph "b" of Claim 1 ("registering the presence of data of a certain type in each data area access system at said information center, followed by the owner of the rights to the stored data, should he wish, defining access rights of third parties to said data at said information center"). Obviously, this offers significant confidentiality beyond that of Schultz et al. Should an authorized physician give unauthorized access to the patient-subscriber's password.

The foregoing significant distinction is made further apparent at Page 24, lines 18 through 22 of Schultz et al. ("Note that the access to these files/databases within (or through) the

institutional server(s) 75', because of security reasons associated with the institutional server(s) 75', may require that the **subscriber obtain permission**, for example, by application to authorities in control of the institutional server(s) 75' at the time of subscribing to the GEMR." Thus, Schultz et al. teaches away from the limitation in which permission to define access rights of third parties to data is limited to the owners of the data rights.

Schultz et al. includes no teaching that would suggest that data is stored only once (i.e. at the originating data area access system). Rather the storage of data obtained from the GEMR server is permitted in the reference in contrast to the limitation of subparagraph "a" of the claimed invention ("in each case storing the data only once in one of said data area access systems not accessible to the owner of the rights"). At page 24, lines 26 through 30 and page 30, lines 21 through 27, Schultz explicitly teaches that the patient-subscriber has permission to access the servers storing his personal medical information. This represents an additional shortcoming (when compared to the claimed invention) of the reference when compared to the claimed invention's more stringent restriction of access to the data area systems. Schultz et al. Does not recognize the significant contribution to data integrity when access to data area access

systems is restricted (e.g. to persons knowledgeable in the field of medical data entry and storage).

In addition to the above-described significant differences between the claimed invention and the system of Schultz et al., other contradictions between the two systems are apparent. For example, at page 4, lines 18 through 27 ("Each subscriber's GEMR has additional files, and/or links, to institutional servers and server files, for the subscriber's hospital discharge summaries, clinical notes, laboratory reports, electrocardiograms, radiology reports, scanned documents, clinical photographs, audio files, and other relevant medical data. In addition to the subscriber, with the subscriber's authorization and an enabling password(s), physicians, healthcare workers, and/or technicians will be able to access these additional files **in order to enter additional medical information** with scanned or embedded data, or to provide services, addresses and pathways (links), e.g., but not limited to, Uniform Resource Locators (URLs) of Uniform Resource identifiers (URIs) which specify resources on the Internet, to locate data." The foregoing clearly contradicts Applicant's teaching of a system in which **the data owner has absolute control** over the data stored on the network and thus this teaching of Schultz et al. teaches away from the applicant's invention.

The other references add little, if any. To an appreciation of the patentable distinctions between the claimed invention and the prior art. As can be seen from the preceding analysis, the claims of the application define significant differences between Applicant's invention and the prior art. Furthermore, the Schultz et al. disclosure is replete with teachings away from significant advantages that are inherent in the claimed invention.

For the foregoing reasons, all presently-pending claims define patentable subject matter. Prompt allowance and issuance of all such claims are therefore earnestly solicited.

Respectfully submitted,

Elliott N. Kramsky
Registration No. 27,812
Attorney for Applicant
5850 Canoga Avenue, Suite 400
Woodland Hills, CA 91367
Ph: (818) 992-5221
Fx: (818) 710-2751